AN OVERLAY NETWORK FOR TRACKING

DENIAL-OF-SERVICE FLOODS

IN UNRELIABLE DATAGRAM DELIVERY NETWORKS

ABSTRACT OF THE DISCLOSURE

An approach for tracking denial-of-service (DoS) flood attacks using an overlay IP (Internet Protocol) network is disclosed. One or more tracking routers form an overlay tracking network over the network of an Internet Service Provider (ISP). The ISP network includes numerous transit routers and edge routers. The tracking routers communicate directly with all the edge routers using IP tunnels. The edge routers within the ISP network perform security diagnostic functions, in part, to identify a DoS flood attack that has been launched by one or more attackers. To track down an attacker, an egress edge router identifies the DoS flood attack datagrams, rerouting these datagrams to the overlay tracking network. The tracking routers perform hop-by-hop input debugging to identify the ingress edge router associated with the source of the DoS flood attack.